CLAIMS

1. A method for distributively and dynamically making a communications network secure, notably of the Internet type, characterized in that it comprises the following steps:

- the step for interconnecting a device (D) between each computer equipment which must be made secure and the communications network,
- the step for intercepting communications between a piece of computer equipment (A) provided with device (D) and the communications network by means of said device to which this piece of equipment is connected,
- the step for obtaining information related to a user (U) of the piece of computer equipment (A) by means of an authentication module (6) associated with device (D),
- the step for defining a security level of the device (D) by means of the authentication module (6) associated with device (D),
- the step for transmitting information related to the user (U) and the security level of the device (D) to an authentication management server (S) connected to the network,
- the step for processing by means of the server (S), said information related to the user and to said security level of the device and for authenticating the user with the help of said information,
- the step for managing the authentications and the security levels by means of the authentication management server (S),

- the step for transmitting security parameters from the server to the network devices,
- the step for storing by means of the devices, said security parameters from the server (S),
- the step for processing by means of the devices, said security parameters issued from the server (S).

(this method enables a distributed and dynamical security to be obtained on a computer network (R), this security is configurable and may develop over time, depending on new needs or new modes of attack)

2. A method according to claim 1, characterized in that the security parameters further comprise:

- a list of authorized computer client/server applications,
- information enabling the devices to analyze the messages related to said client/server applications.

3. A method according to claim 2, characterized in that it further comprises the following steps:

- the step for analyzing by means of the device (D), the messages related to said client/server applications,
- the step for filtering by means of the device (D) the messages related to said client/server applications,
- the step for altering by means of the device (D) the messages related to said client/server applications.

(this method allows a lock to be obtained (commonly called a firewall) managed by a server and distributed over all the network. This lock further has particular properties for each piece of computer equipment

equipped with the device)

4. A method according to claim 1, characterized in that the security parameters further comprise:

- a list of pieces of computer equipment which the user (U) is authorized to communicate with.

5. A method according to claim 4, characterized in that it further comprises the following steps:

- the step for allowing the device (D) transmit messages between the piece of computer equipment (A) and computer equipment which the user (U) is authorized to communicate with,
- the step for blocking with the device (D) messages between the piece of computer equipment (A) and computer equipment which the user (U) is not authorized to communicate with.

(this method enables a partitioning system to be designed for the network components)

6. A method according to claim 1, characterized in that it further comprises the following steps:

- the step for customizing the device (D) with the help of a private encipherment key provided by means of the authentication module (6),
- the step for storing by means of the server (S), all public encipherment keys associated with private encipherment keys which customize the devices.

7. A method according to claim 6, characterized in that the security parameters further comprise:

- a list of computer equipment which the user (U) is authorized to communicate with, in an enciphered way,
- the public encipherment key of each piece of computer equipment which the user (U) is

authorized to communicate with, in an enciphered way.

8. A method according to claim 7, characterized in that it further comprises the following steps:

- the step for enciphering by means of device (D), communications by combining the private encipherment key of said device (D) with the public encipherment key of the piece of computer equipment which the user (U) is authorized to communicate with, in an enciphered way.

(this method provides encipherment of communications between two devices. This encipherment depends on each pair of devices)

9. A system for distributively and dynamically making a communications network secure, notably of the Internet type, characterized in that it comprises:

- a device (D) interconnected between each piece of computer equipment which is to be made secure and the communications network,
- said device including two input/output interfaces for intercepting communications between a piece of computer equipment (A) to which it is connected and the communications network,
- said device further including an authentication module (6) for obtaining information related to a user (U) of the computer equipment (A) and for defining a security level of said device,
- said device including means for transmitting information related to the user (U) and to the security level of the device,
- an authentication management server (S) connected to the network including processing means for processing said information and said security

level and for authenticating the user with the help of said information,

- said server including management means for managing the authentications and the security levels,
- said server (S) including means for transmitting security parameters, to the devices of the network,
- said devices (D) including storage means for storing said security parameters,
- said devices (D) including processing means for processing said security parameters.

10. A system according to claim 9, characterized in that the security parameters comprise:

- a list of authorized computer client/server applications,
- information enabling the devices to analyze the messages related to said client/server applications.

11. A system according to claim 10, characterized in that the processing means of the device comprise:

- means for analyzing the messages related to said client/server applications,
- means for filtering the messages related to said client/server applications,
- means for altering messages related to said client/server applications.

12. A system according to claim 9, characterized in that the security parameters further comprise:

- a list of computer equipment which the user (U) is authorized to communicate with.

13. A system according to claim 12, characterized in that said processing means of the device further comprise:

- means for allowing messages to be transmitted between the piece of computer equipment (A) and computer equipment which the user (U) is authorized to communicate with,
- means for blocking messages between computer equipment (A) and computer equipment which the user (U) is not authorized to communicate with.

14. A system according to claim 9, characterized in that

- the authentication module associated with the customized device by means of a private encipherment key which customizes the device with which it is associated,
- the server (S) stores all the public encipherment keys associated with private encipherment keys which customize the devices.

15. A system according to claim 14, characterized in that the security parameters further comprise:

- a list of computer equipment which the user (U) is authorized to communicate with, in an enciphered way,
- the public encipherment key of each piece of computer equipment which the user (U) is authorized to communicate with, in an enciphered way.

16. A system according to claim 15, characterized in that the device further comprises:

- an encipherment module for enciphering communications by combining the private encipherment key of device (D) with the public encipherment key of the piece of computer equipment with which the user (U) is authorized to communicate with, in an enciphered way.

17. A server for distributively and dynamically making a communications network secure, notably of the Internet type, characterized in that it comprises:

- processing means for processing the information from a device (D) and related to a user (U) of a piece of computer equipment (A) to which this device (D) is connected,
- said processing means enabling the user (U) to be identified with the help of said information,
- management means for managing the authentications,
- transmission means for transmitting security parameters to the network devices.

18. A server according to claim 17, characterized in that the security parameters comprise:

- a list of authorized computer client/server applications,
- information enabling the devices to analyze the messages related to said client/server applications.

19. A server according to claim 17, characterized in that the security parameters further comprise:

- a list of computer equipment which the user (U) is authorized to communicate with.

20. A server according to claim 17, characterized in that it comprises:

- storage means for storing all the public encipherment keys associated with private encipherment keys which customize the devices.

21. A server according to claim 20, characterized in that the security parameters further comprise:

- a list of computer equipment which the user (U) is authorized to communicate with, in an enciphered way,

- the public encipherment key of each piece of computer equipment which the user (U) is authorized to communicate with, in an enciphered way.

22. Device for making a communications network secure, interconnected between each piece of computer equipment which is to be made secure and said network and characterized in that it comprises:

- two input/output interfaces for intercepting communications between computer equipment (A) to which it is connected and the communications network,
- an authentication module (6) for obtaining information related to a user (U) of the computer equipment (A) and for defining the security level of said device,
- means for transmitting information related to user (U) and the device's security level to an authentication management server (S),
- storage means for storing security levels from the server (S),
- processing means for processing said security levels from the server (S).

23. A device according to claim 22, characterized in that the security parameters comprise:

- a list of authorized computer client/server applications,
- information enabling the devices to analyze the messages related to said client/server applications.

24. A device according to claim 23, characterized in that said processing means of the device comprise:

- means for analyzing the messages related to said

client/server applications,

- means for filtering the messages related to said client/server applications,
- means for altering messages related to said client/server applications.

25. A device according to claim 22, characterized in that the security parameters further comprise:

- a list of computer equipment which the user (U) is authorized to communicate with.

26. A device according to claim 25, characterized in that said processing means of the device comprise:

- means for allowing messages to be transmitted between a piece of computer equipment (A) and the computer equipment which the user (U) is authorized to communicate with,
- means for blocking messages between a piece of computer equipment (A) and computer equipment which the user (U) is unauthorized to communicate with.

27. A device according to claim 22, characterized in that the authentication module associated with said device further provides:

- a private encipherment key which customizes said device(D).

28. A device according to claim 27, characterized in that the security parameters further comprise:

- a list of computer equipment which the user (U) is authorized to communicate with, in an enciphered way,
- the public encipherment key of each piece of computer equipment which the user (U) is authorized to communicate with, in an enciphered way.

Q5

29. A device according to claim 28, characterized in that it further comprises:

- an encipherment module for enciphering communications by combining the private encipherment key of said device (D) with the public encipherment key of the computer equipment which the user (U) is authorized to communicate with, in an enciphered way.